SECTIGO

A WHITEPAPER FROM SECTIGO

Combating Attacks: Best Practices in Securing Your Digital Identity

By Lindsay Kent, Sectigo

Malware attacks, cybercrime, cyberterrorism and related threats are increasing on a daily basis. So too is the defense of these attacks, as Certificate Authorities (CA) implement security measures that stay ahead of an attacker's next step. There have been service-affecting breaches of security of systems and processes in the past. CAs need to continuously and diligently find new methods to proactively prevent the threats.

What You Should Expect From Your CA

As the world's largest commercial certification authority, Sectigo is proactively monitoring for potential threats and attacks. Additionally, we are working hand-in-hand with government agencies, browsers and customers, all of whom are keeping us apprised of new attack threats. In fact, Sectigo frequently knows about and has resolved a threat before an enterprise customer hears about it, offering a level of security the enterprise cannot achieve on their own.

As an example, in 2011, four CAs were attacked by an organization that was based in the middle east, hoping to impersonate legitimate web sites. The attacker used malware running on a partner's desktop that stole the user name and password to issue 9 publicly trusted SSL certificates. While our monitoring tools allowed us to identify the infraction and revoke all 9 certificates within 2 hours, we learned from it, implementing the following changes:

- While the Sectigo facility itself was not breached, the company implemented the preventative measure of a strong smart card – certificate-based authentication, augmenting the use of user name and password. This credential cannot be duplicated or stolen.

- All SSL certificate issuance must first prove control of the domain for which the certificate is issued.

- Sectigo implemented changes that no longer allow the 3rd party Registration Authority to perform the Domain Control Validation from their facility. All SSL certificate issuance uses the Domain Control Validation hosted by Sectigo, which is protected by our facility's WebTrust audited computer and physical security.

Ensuring Your CA is Secure

When considering a CA, be sure they've implemented baseline requirements as defined below.

Follow CA/Browser Forum Baseline Requirements

The Certification Authority and Browser Forum developed rules that every Certification Authority must meet. These include:

- All information contained within the certificate must be validated to be true through a strict authentication process.
- The minimum levels of cryptographic strength that must be used to protect the integrity of the certificate and private key from evolving threats.
- CA security, certificate revocation mechanisms, audit requirements, liability, privacy, confidentiality, and delegation of authority.

Conduct Annual Audits – Both WebTrust and SOC 3

Annual audits are crucial to CA security. Every CA has to do a WebTrust audit, but the SOC 3 audit is optional. Sectigo is both WebTrust certified and SOC 3 compliant. Sectigo consistently looks to go above and beyond the minimum requirements.

WebTrust

The WebTrust for Certification Authorities program was developed to increase consumer confidence in the Internet as a vehicle for conducting e-commerce and to increase consumer confidence in the application of PKI technology. Sectigo undergoes an annual audit from Ernst & Young, which validates:

- The Certification Authority (CA) discloses its SSL Certificate practices and procedures and its commitment to provide SSL Certificates in conformity with the applicable CA/ Browser Forum Requirements.

- Subscriber information was properly collected, authenticated and verified, the integrity of keys and certificates it manages is established and protected throughout their life cycles.

- Logical and physical access to CA systems and data is restricted to authorized individuals, the continuity of key and certificate management operations is maintained, and CA systems development, maintenance and operations are properly authorized and performed to maintain CA systems integrity.

- The Certification Authority (CA) maintains effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum.

Annual Service Organization Control 3

The SOC3 report is published to confirm that the security controls for this cloud service have been examined by an independent accountant. Sectigo undergoes an annual audit that is performed by Ernst&Young, which validates whether Sectigo maintained effective controls over its system as it relates to:

- The security principle refers to the protection of the system resources through logical and physical access control measures. Controls over the security of a system prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or unauthorized removal of data or system resources, misuse of software, and improper access to, or use of, alteration, destruction, or disclosure of information.

- The availability principle refers to the accessibility of the system, products, or services as committed by contract, service-level agreement, or other agreements. Addresses whether the system includes controls to support system accessibility for operation, monitoring, and maintenance.

- The processing integrity principle refers to the completeness, validity, accuracy, timeliness, and authorization of system processing. Processing integrity addresses whether the system achieves its aim or the purpose for which it exists, and whether it performs its intended function in an unimpaired manner, free from unauthorized or inadvertent manipulation.

- The confidentiality principle addresses the system's ability to protect information designated as confidential in accordance with the organization's commitments and requirements through its final disposition and removal from the system.

Customer Involvement is Key

A key ingredient to the prevention of attacks, and the mitigation of those attacks, is to involve the customer in a prompt and responsible manner. Sectigo's threat response team takes the lead in assessing the threat, and when necessary ensures the customer is aware of the threat, and any mitigating factors they can implement to prevent or limit damage while also identifying possible intrusions.

While the protection of the private key relies on systems implemented by the customers, Sectigo offers our expertise on how to protect the private key from theft.

Safeguarding Your Enterprise Against Future Attacks

Unfortunately, there will continue to be attacks on CAs and their customers. However, by working with a trusted CA that is proactive, undergoes routine annual audits, and works closely with customers is a key to protecting your enterprise. CAs are here to help the certificate users by providing secure and authenticated ways for them to interact with their consumers, employees and devices.

Enterprise Certificate Authority

The same audits and controls put in place for publicly trusted SSL are used to provide secure practices for the enterprise certificate authority. Whether the usage is user certificates, device/internet of things certificates or SSL/TLS, the enterprise can trust their digital identities.

About

Sectigo provides web security products that help customers protect, monitor, recover, and manage their web presence and connected devices. As the largest commercial Certificate Authority trusted by enterprises globally for more than 20 years, with more than 100 million SSL certificates issued in over 200 countries, Sectigo has the proven performance and experience to meet the growing needs for securing today's digital landscape.
For more information, visit **www.sectigo.com.**

